Extensions of the Levine-Nahikian Method for Constructing Involutory Matrices

Randall E. Cline
Department of Mathematics and Computing Center
University of Tennessee
Knoxville, Tennessee 37996

and

Robert M. McConnel
Department of Mathematics
University of Tennessee
Knoxville, Tennessee 37996

Submitted by Robert J. Plemmons

ABSTRACT

Various characterizations for sums of matrices over arbitrary fields to be involutions are established. Applications of these results in constructing involutions of matrices with elements from finite fields are considered.

1. INTRODUCTION

Let A denote an n by n matrix over a ring with identity. Such a matrix is called involutory if $A^2 = I$, where I is the n by n identity matrix. Studies of involutory matrices and special classes of involutory matrices have frequently appeared in the literature; e.g., see [1–4,6,8,9,18,19]. These studies are motivated partly by the use of involutory matrices in the study of particular algebraic structures and by the importance of involutory matrices and groups of involutory matrices in algebraic cryptography; e.g., see [5,7,10–13]. Techniques for constructing involutory matrices have been presented in [3,14–17]. In particular, in [16], an explicit general formula for an involutory matrix over a commutative ring with identity is obtained; this formula results from the construction procedure for involutory matrices over the ring of integers modulo m. Other construction methods seem to require solving a matrix

52 Vanderbilt Ave., New York, NY 10017 0024-3795/84/$3.00

equation or applying similarity transformations to a matrix of a specific type. In this paper we consider various characterizations of involutory matrices over a field and obtain a method for constructing involutory matrices.

Given an arbitrary matrix H over any field, Levine and Nahikian [17] established necessary and sufficient conditions for H to be involutory, and counted the number of dissimilar involutions of a given size. Their results, which we summarize and write in a single concise form in Section 2, show that $H^2 = I$ if and only if H can be written as

$$H = I \pm R, \tag{1.1}$$

where the sign and the conditions on R depend upon the characteristic of the field. As they then illustrate with numerical examples, these forms for H can be used in constructing involutions over finite field.

The purpose of this paper is to show, more generally, that involutions can be constructed by replacing I in (1.1) with an arbitrary tripotent matrix P, that is, we write

$$H = P \pm R, \tag{1.2}$$

where $P^3 = P$, and consider conditions on R to have $H^2 = I$. For the special case $P^2 = I$, our results thus provide direct methods for constructing one involution from another nontrivial involution P. Having summarized the Levine-Nahikian theorems in Section 2, we establish the main results in Section 3, and discuss how they can be used for computational purposes in Section 4. We then conclude in Section 5 with numerical examples. Throughout the discussion it is assumed that all matrices in any sum or product have elements from a field $\mathcal{F}$ with characteristic p; unless otherwise stated, $p = 0$ or p is an arbitrary prime. In every theorem the only assumption on p will be either $p \neq 2$ or $p \neq 3$, or both, and these restrictions will be resolved as special cases whenever possible.

2. A COMBINED FORM FOR THE LEVINE-NAHIKIAN RESULTS

If H is any n by n involution over any field of characteristic $p \neq 2$, then, excluding the trivial cases $H = \pm I_n$, H is similar to a diagonal matrix

$$\begin{bmatrix} I_r & 0 \\ 0 & -I_s \end{bmatrix},$$

where s, the number of eigenvalues $\lambda = -1$, is called the signature of H

[8, 17]. Then Levine and Nahikian showed [17, Theorem 1] that a necessary and sufficient condition for H to be a nontrivial involution with signature s is

$$H = I_n - Q_2 P_2, \tag{2.1}$$

where Q_2 is n by s, P_2 is s by n, and $P_2 Q_2 = 2I_s$, or alternatively,

$$H = Q_1 P_1 - I_n, \tag{2.2}$$

where Q_1 is n by r, P_1 is r by n, and $P_1 Q_1 = 2I_r$ with $r + s = n$. In contrast, H an involution when $p = 2$ implies either $H = I_n$ or H is similar to the matrix

$$J = \begin{bmatrix} I_r & 0 \\ 0 & K_{2s} \end{bmatrix}$$

with K_{2s} the direct sum of s matrices of the form

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

and $r + 2s = n$, $0 < s \leqslant n/2$. For $H \neq I_n$ in this case, s is again called the signature of H, and Levine and Nahikian showed (Theorem 2) that a necessary and sufficient condition for H to be a nontrivial involution with signature s is

$$H = I_n + Q_2 P_2, \tag{2.3}$$

where Q_2 is n by s and P_2 is s by n, both with rank s, and $P_2 Q_2 = 0$. Having characterized all nontrivial involutions in these theorems, the authors then noted (Theorem 3) that the number $N(\mathscr{F}, n)$ of classes of dissimilar n by n involutory matrices over $\mathscr{F}$ is given by

$$N(\mathscr{F}, n) = \begin{cases} 1 + n & \text{if } p \neq 2, \\ 1 + [n/2] & \text{if } p = 2. \end{cases}$$

To motivate the starting point for our discussion in Section 3, we observe first that since H is an involution if and only if $(-H)^2 = I$, the alternative form for H in (2.2) reduces at once to (2.1). Now for any involution H in (2.1), $P_2 Q_2 = 2I_s$ implies P_2 has full row rank and Q_2 has full column rank, that is,

the same condition on rank required in (2.3); and if $R = Q_2P_2$, then $R^2 = 2R$. But in a field with characteristic $p = 2$ we have $R^2 = 0$, which holds for $R = Q_2P_2$ in (2.3). Conversely, noting that any n by n matrix R with rank s has a full rank factorization $R = Q_2P_2$ with $P_2Q_2 = 2I_s$ if $R^2 = 2R$ and $P_2Q_2 = 0$ if $R^2 = 0$ establishes the following combined form of Theorems 1 and 2 from Levine and Nahikian.

THEOREM (Levine-Nahikian). *Let H be an arbitrary matrix over any field. Then a necessary and sufficient condition for H to be an involution with signature s is*

$$H = I - R \tag{2.4}$$

where R has rank s and

$$R^2 = 2R. \tag{2.5}$$

That the conditions to have H involutory in this theorem can be written in alternative ways is easily seen: For example, replacing R by $-R$, (2.4) becomes

$$H = I + R, \tag{2.6}$$

to correspond directly to (2.3), in which case (2.5) becomes

$$(-R)^2 = -2R. \tag{2.7}$$

In addition, observe that in any field with characteristic $p \neq 2$, $R = 2P_2$ with P_2 an arbitrary idempotent matrix satisfies (2.5). Given our goal of extending the Levine-Nahikian method for constructing involutory matrices, we begin in Section 3 by considering matrices of the form $P_1 + P_2$ with $P_1^3 = P_1$ and $P_2^2 = P_2$. To obtain involutions in fields with characteristic $p \neq 2$, we then consider matrices $P_1 + \alpha P_2$ with $P_1^2 = I$, $P_2^2 = P_2$, and α an arbitrary scalar, where α is introduced to yield simple sets of conditions so that $(P_1 + \alpha P_2)^2 = I$. It is shown, however, that excluding the trivial special case $\alpha = 0$, then $\alpha = \pm 2$, and αP_2 assumes the role of R in (2.5) or (2.7).

3. MAIN RESULTS

In this section we establish various characterizations for involutions which generalize the combined form of the Levine-Nahikian theorem. Since involu-

tions are obtained, these results can always be reduced to obtain the form for H in (2.4) where R satisfies (2.5), and such reductions will be noted below. For subsequent computational purposes, however, the characterizations given here are more appropriate.

It will follow as a special case of Theorem 1 that there are two involutions associated with any tripotent matrix P_1.

THEOREM 1. *Let P_1 and P_2 be arbitrary matrices over any field with $P_1^3 = P_1$ and $P_2^2 = P_2$. Then a sufficient condition to have $P_1 + P_2$ involutory is that there exists a matrix N such that*

$$P_1^2 + P_2 = I + N \tag{3.1}$$

and

$$P_1N + NP_1 = -N. \tag{3.2}$$

Conversely, these conditions are also necessary in any field of characteristic $p \neq 3$.

Proof. If N is any matrix such that (3.1) and (3.2) hold, then

$$P_1P_2 = P_1N, \qquad P_2P_1 = NP_1, \tag{3.3}$$

and so

$$(P_1 + P_2)^2 = P_1^2 + P_1P_2 + P_2P_1 + P_2 = I + N + P_1N + NP_1 = I.$$

Conversely, if $P_1 + P_2$ is an involution, then

$$P_1^2 + P_1P_2 + P_2P_1 + P_2 = I \tag{3.4}$$

implies

$$P_1^2P_2 + P_1P_2P_1 + P_1P_2 = 0 \tag{3.5}$$

and

$$P_1P_2P_1 + P_2P_1^2 + P_2P_1 = 0.$$

Hence

$$P_1^2P_2 + P_1P_2 = P_2P_1^2 + P_2P_1 = -P_1P_2P_1 = -P_1^2P_2P_1 = -P_1P_2P_1^2, \quad (3.6)$$

where the last two equalities follow from $P_1(P_1^2 + P_1) = P_1^2 + P_1 = (P_1^2 + P_1)P_1$. Therefore, with

$$P_1^2P_2P_1 + P_1P_2P_1^2 + P_1P_2P_1 = 0$$

from (3.5), and $p \neq 3$,

$$P_1P_2P_1 = 0. \quad (3.7)$$

Thus (3.6) implies

$$P_1P_2 = -P_1^2P_2, \qquad P_2P_1 = -P_2P_1^2, \quad (3.8)$$

and (3.4) becomes

$$P_1^2 + P_2 = I + P_1^2P_2 + P_2P_1^2. \quad (3.9)$$

Taking $N = P_1^2P_2 + P_2P_1^2$ in (3.9) gives (3.1), and (3.2) follows at once from (3.7) and (3.8). ■

Observe that, with N defined in this manner,

$$P_1^2N + NP_1^2 = N \quad (3.10)$$

also follows from (3.7) and (3.8).

COROLLARY 2. *If P_1 and P_2 are arbitrary matrices over any field of characteristic $p \neq 3$ with $P_1^3 = P_1$ and $P_2^2 = P_2$, then $P_1 + P_2$ an involution implies $P_1^2 - P_2$ is an involution.*

Proof. If $(P_1 + P_2)^2 = I$, then (3.8) holds and

$$\begin{aligned}(P_1^2 - P_2)^2 &= P_1^4 + P_2^2 - P_1^2P_2 - P_2P_1^2 \\ &= P_1^2 + P_2^2 + P_1P_2 + P_2P_1 \\ &= (P_1 + P_2)^2 = I.\end{aligned}$$

■

It should be noted that the involutions provided by Theorem 1 and Corollary 2 are generally distinct. Indeed, if

$$P_1 + P_2 = P_1^2 - P_2, \tag{3.11}$$

then $P_1 = P_1^2$, by use of (3.7) when $p \neq 2,3$. Hence $P_2 = 0$ for $p \neq 2$, and thus $P_1 = I$ as $P_1 + P_2 = P_1$ is an involution. On the other hand, for $p = 2$ and $P_1^2 = P_1$, (3.1) gives $P_1 + P_2 = I + N$, which will be shown (Corollary 4) to be a standard form for an involution in this case.

That the involutions in Theorem 1 and Corollary 2 may be written in the form of the Levine-Nahikian theorem can be shown in the following manner: Observe first that with both P_1^2 and P_2 idempotent in (3.1), then

$$P_2 = P_2^2 = \left(I - P_1^2 + N\right)^2 = P_2 + N^2,$$

by (3.10), gives

$$N^2 = 0 \tag{3.12}$$

[which can be verified directly for the choice of N used to obtain (3.1) from (3.9) by noting that $P_2 P_1 P_2 = 0$]. Also, using (3.1) to write

$$P_1 + P_2 = I + P_1 - P_1^2 + N,$$

then with $(P_1 - P_1^2)^2 = -2(P_1 - P_1^2)$ and

$$N\left(P_1 - P_1^2\right) + \left(P_1 - P_1^2\right)N = -2N,$$

by (3.2) and (3.10), $P_1 + P_2$ has the form in (2.6), where $R = P_1 - P_1^2 + N$ satisfies (2.7). In a similar manner,

$$P_1^2 - P_2 = I - 2P_2 + N \tag{3.13}$$

gives the form in (2.4), where $R = 2P_2 - N$. Then R satisfies (2.5), since the relation

$$R^2 = 4P_2 - 2P_2N - 2NP_2 = 2R$$

follows by noting that

$$NP_1^2 + NP_2 = N$$

and

$$P_1^2 N + P_2 N = N,$$

by use of (3.1), combine with (3.10) to give $P_2 N + N P_2 = N$. That $P_1 + P_2$ and (3.13) have the correct forms in a field of characteristic $p = 2$ follows easily.

It is shown in the following corollary that assuming $P_1^2 = I$ in Theorem 1 yields only trivial involutions. Here and in all of the remaining results in this section, sufficiency follows at once, so that we only prove necessity in each case.

COROLLARY 3. *Let P_1 and P_2 be arbitrary matrices over any field with $P_1^2 = I$ and $P_2^2 = P_2$. Then a sufficient condition to have $P_1 + P_2$ involutory is $P_2 = 0$. Conversely, $P_2 = 0$ is also a necessary condition in any field of characteristic $p \neq 3$.*

Proof. With $P_1 + P_2$ an involution, $P_2 = N$ by (3.1). Hence

$$P_1 P_2 + P_2 P_1 = -P_2, \tag{3.14}$$

from (3.2), so that

$$P_1 P_2 + P_2 P_1 P_2 = -P_2$$

and

$$P_2 P_1 P_2 + P_2 P_1 = -P_2,$$

which give $P_1 P_2 = P_2 P_1$. Therefore,

$$2 P_1 P_2 = -P_2 \tag{3.15}$$

by (3.14), and the conclusion follows if $p = 2$. In contrast, for $p \neq 2$, (3.15) implies each column of P_2 is an eigenvector of P_1 for eigenvalue $\lambda = -(2)^{-1}$. But P_1 has only eigenvalues $\lambda = \pm 1$. ∎

The next corollary includes the previously noted form for $P_1 + P_2$ when (3.11) holds in a field of characteristic $p = 2$.

COROLLARY 4. *Let P_1 and P_2 be arbitrary matrices over any field with $P_1^2 = P_1 \neq 0$ and $P_2^2 = P_2$. Then a sufficient condition to have $P_1 + P_2$ involu-*

tory is

$$P_1 + P_2 = I + N, \tag{3.16}$$

where $N^2 = 0$ *if the field has characteristic* $p = 2$, *and* $N = 0$ *if* $p \neq 2$. *Conversely, these conditions are necessary in any field of characteristic* $p \neq 3$.

Proof. If $P_1 + P_2$ is an involution and $p = 2$, then (3.1) gives (3.16) where $N^2 = 0$ from (3.12). Now if $p \neq 2,3$, it follows from (3.2) that

$$P_1NP_1 + NP_1 = -NP_1,$$

and thus

$$P_1NP_1 = -2NP_1.$$

Hence $NP_1 = 0$, since P_1 has only eigenvalues $\lambda = 0$ and $\lambda = 1$. By a similar type of argument applied to

$$P_1N + P_1NP_1 = -P_1N,$$

$P_1N = 0$. Thus $N = 0$ from (3.2). ■

That the assumption $p \neq 3$ is needed in the proofs of necessity in both Corollaries 3 and 4 is apparent by noting that if $p = 3$, $(I + P_2)^2 = I$ for any idempotent matrix P_2.

Having shown in Corollary 3 that given any matrix P_1 with $P_1^2 = I$, there exists no nontrivial idempotent matrix P_2 for which $P_1 + P_2$ is involutory, we next introduce an arbitrary scalar, α, and consider matrices of the form $P_1 + \alpha P_2$ where $P_2 \neq 0$. For completeness of the characterizations, however, the trivial special case $\alpha = 0$ is included in each of the following results. As in [17], it is convenient to consider the cases $p \neq 2$ and $p = 2$ separately.

THEOREM 5. *Let* P_1 *and* P_2 *be arbitrary matrices over any field of characteristic* $p \neq 2$ *with* $P_1^2 = I$ *and* $P_2^2 = P_2 \neq 0$. *Then* $P_1 + \alpha P_2$ *is an involution if and only if one of the following conditions holds:*

(i) $\alpha = 0$,
(ii) $\alpha = -2$, $P_1P_2 = P_2P_1 = P_2$,
(iii) $\alpha = 2$, $P_1P_2 = P_2P_1 = -P_2$.

Proof. If $P_1 + \alpha P_2$ is an involution, then

$$\alpha(P_1P_2 + P_2P_1) + \alpha^2 P_2 = 0 \tag{3.17}$$

implies

$$\alpha(P_2 + P_1P_2P_1) + \alpha^2 P_1P_2 = 0$$

and

$$\alpha(P_1P_2P_1 + P_2) + \alpha^2 P_2P_1 = 0.$$

Excluding the special case $\alpha = 0$ that gives (i), then $P_1P_2 = P_2P_1 \neq 0$, where the inequality holds because otherwise $P_2 = 0$. Now (3.17) becomes

$$2P_1P_2 + \alpha P_2 = 0,$$

which combines with

$$2P_2 + \alpha P_1P_2 = 0$$

to yield $(\alpha^2 - 4)P_2 = 0$, and thus the conditions in (ii) and (iii). ∎

Replacing the condition $P_2^2 = P_2$ by $P_2^2 = 0$ immediately gives an analog of Theorem 5 which includes the case $p = 2$.

THEOREM 6. *Let P_1 and P_2 be arbitrary matrices over any field with $P_1^2 = I$ and $P_2^2 = 0 \neq P_2$. Then $P_1 + \alpha P_2$ is an involution if and only if one of the following conditions holds:*

(i) $\alpha = 0$,
(ii) $\alpha \neq 0$, $P_1P_2 + P_2P_1 = 0$.

We remark at this point that there does not appear to be a concise way to combine Theorem 5 and Theorem 6 with $p = 2$ and $\alpha = 1$ to correspond to the statement of the Levine-Nahikian results in Section 2.

As will be discussed in Section 4, given a matrix P_1 with $P_1^2 = I$, the conditions in Theorems 5 and 6 can be used directly to construct matrices P_2 to obtain nontrivial involutions.

We conclude this section by returning to the involution $P_1 + P_2$ in Corollary 4 with both P_1 and P_2 idempotent, and generalize this result by

again introducing an arbitrary scalar α to write $P_1 + \alpha P_2$. The various sets of conditions on P_1, P_2, and α, although clearly not useful for computational purposes, completely characterize such involutory matrices in forms similar to those in Theorems 5 and 6. Here again we only establish necessity. Also, since the conditions for $p = 3$ and $p \neq 3$ differ somewhat, it is convenient to treat these cases separately.

THEOREM 7. *Let P_1 and P_2 be arbitrary matrices over any field of characteristic $p \neq 3$ with $P_1^2 = P_1 \neq 0$ and $P_2^2 = P_2 \neq 0$. Then $P_1 + \alpha P_2$ is an involution if and only if one of the following conditions holds:*

(i) $\alpha = 0, -2, P_1 = I$,
(ii) $\alpha = 1, P_1 + P_2 = I$,
(iii) $\alpha = -1, P_1 + P_2 = I + N, P_2N + NP_2 = N, N^2 = 0$ *for some matrix* N.

Proof. With $P_1 + \alpha P_2$ an involution,

$$P_1 + \alpha(P_1P_2 + P_2P_1) + \alpha^2 P_2 = I. \tag{3.18}$$

Moreover, using (3.18),

$$\alpha(P_1P_2 + P_1P_2P_1) + \alpha^2 P_1P_2 = 0 \tag{3.19}$$

and

$$\alpha(P_1P_2P_1 + P_2P_1) + \alpha^2 P_2P_1 = 0$$

so that

$$(1+\alpha)P_1P_2 = (1+\alpha)P_2P_1 \tag{3.20}$$

when $\alpha \neq 0$.

Now $\alpha = 0$ implies $P_1 = I$, so that (i) holds. On the other hand, if $\alpha \neq 0$, then (3.20) implies $\alpha = -1$ or $P_1P_2 = P_2P_1$. If $\alpha = -1$, then $P_1P_2P_1 = 0$ from (3.19) and, dually, $P_2P_1P_2 = 0$ by use of (3.18). Whereupon, writing (3.18) as

$$P_1 + P_2 = I + P_1P_2 + P_2P_1, \tag{3.21}$$

taking $N = P_1P_2 + P_2P_1$ gives $P_2N + NP_2 = N$ and $N^2 = 0$ as in (iii).

Thus suppose $\alpha \neq -1$ and $P_1P_2 = P_2P_1$. If $P_1P_2 \neq 0$, then (3.18) becomes

$$P_1 + 2\alpha P_1P_2 + \alpha^2 P_2 = I \tag{3.22}$$

to give

$$P_1P_2 + 2\alpha P_1P_2 + \alpha^2 P_1P_2 = P_1P_2,$$

which implies $\alpha = -2$. Consequently, with $p \neq 3$, (3.22) yields $P_1P_2 = P_2$, and thus $P_1 = I$ as in (i). If $P_1P_2 = 0$, then

$$P_1 + \alpha^2 P_2 = I \tag{3.23}$$

from (3.18) implies $\alpha^2 P_2 = P_2$, so that $\alpha = \pm 1$. Hence $\alpha = 1$, and (3.23) gives (ii). Finally, note that if $p = 2$, then $-1 = 1$ and condition (ii) is included in condition (iii). ■

The corresponding result when $p = 3$ is given in Theorem 8 where portions of the proof of Theorem 7 hold without modification.

THEOREM 8. *Let P_1 and P_2 be arbitrary matrices over any field of characteristic $p = 3$ with $P_1^2 = P_1 \neq 0$ and $P_2^2 = P_2 \neq 0$. Then $P_1 + \alpha P_2$ is an involution if and only if one of the following conditions holds:*

(i) $\alpha = 0$, $P_1 = I$,
(ii) $\alpha = 1$, $P_1 + P_2 = I + M$, $M^2 = M$ *for some matrix* M,
(iii) $\alpha = 2$, $P_1 + P_2 = I + N$, $P_2N + NP_2 = N$, $N^2 = 0$ *for some matrix* N.

Proof. From the proof of Theorem 7 one obtains (i) when $\alpha = 0$ and (iii) when $\alpha = -1 = 2$ in characteristic 3. Thus suppose that $\alpha \neq 0$, $\alpha \neq 2$, and $P_1P_2 = P_2P_1$. If $P_1P_2 \neq 0$, then (3.22) implies $\alpha = 1$ and thus (3.22) can be written as

$$P_1 + P_2 = I + P_1P_2.$$

Then $M = P_1P_2$ is idempotent and (ii) results. If $P_1P_2 = 0$, then (3.23) implies $\alpha = 1$ and thus (3.23) gives $P_1 + P_2 = I$, which is (ii) with $M = 0$. ■

4. COMPUTATIONAL PROCEDURES

Given an arbitrary involution P_1 over any field of characteristic $p \neq 2$, it follows at once that columns of the matrices $I + P_1$ and $I - P_1$ are right

eigenvectors of P_1 and that rows of these matrices are left eigenvectors of P_1 corresponding, respectively, to eigenvalues $\lambda = 1$ and $\lambda = -1$. Moreover, since the partitioned matrix $[I + P_1, I - P_1]$ has full row rank, eigenvectors obtained in this manner using either rows or columns of $I + P_1$ and $I - P_1$ together form complete sets. In contrast, I is the only involution in a field of characteristic $p = 2$ with a complete set of eigenvectors, and if P_1 is an involution with signature $s > 0$, then again rows and columns of $I + P_1$ are left and right eigenvectors of P_1, but now P_1 has s generalized eigenvectors corresponding to the two by two diagonal blocks of the submatrix K_{2s} introduced in Section 2. As will be seen in the proofs of Theorems 9, 10, and 11, these observations on the eigenvector structure of involutions can be used directly in the construction of dissimilar classes of involutions.

THEOREM 9. *Let P_1 be an arbitrary n by n involution with signature s, $0 < s < n$, over any field of characteristic $p \neq 2$. Then there exists at least one idempotent matrix P_2 with rank one such that $P_1 + 2P_2$ is involutory and the signature of $P_1 + 2P_2$ is $s - 1$. Such a P_2 may be obtained by setting $P_2 = (vu)^{-1}uv$, where v is any nonzero row of $I - P_1$, say the ith, and u is any column of $I - P_1$, say the kth, for which the ith component of u is nonzero. Dually, there exists at least one idempotent matrix P_2 with rank one such that $P_1 - 2P_2$ is involutory and the signature of $P_1 - 2P_2$ is $s + 1$; moreover, such a P_2 may be obtained in the same manner as before except that u and v are chosen from $I + P_1$.*

Proof. P_1 with signature s implies P_1 has s eigenvalues $\lambda = -1$ and $n - s$ eigenvalues $\lambda = 1$, and with $0 < s < n$, both $I + P_1 \neq 0$ and $I - P_1 \neq 0$.

By Theorem 5(iii), $P_1 + 2P_2$ is involutory for any idempotent matrix P_2 if and only if

$$P_1P_2 = P_2P_1 = -P_2, \tag{4.1}$$

so that each row and column of P_2 must be a left and right eigenvector of P_1, respectively, for $\lambda = -1$. Therefore, if v is any nonzero row of $I - P_1$ with components $v_1, \ldots, v_n$, and u is any column of $I - P_1$ with a component $v_k \neq 0$ for some k, then $uv \neq 0$, and $vu \neq 0$, since $(I - P_1)^2 = 2(I - P_1)$ and $p \neq 2$. Hence the matrix $P_2 = (vu)^{-1}uv$ is idempotent and satisfies (4.1). In addition, with P_2 formed in this manner, $P_2u = u$. Now for any eigenvector x of P_1 for $\lambda = 1$,

$$P_2x = P_2P_1x = -P_2x$$

by (4.1), so that $P_2x = 0$. Thus, for each such eigenvector x,

$$(P_1 + 2P_2)x = x,$$

and with $P_1u = -u$, by the method of choosing u,

$$(P_1 + 2P_2)u = u.$$

Hence, $P_1 + 2P_2$ has $n - s + 1$ linearly independent eigenvectors corresponding to $\lambda = 1$, so the signature of $P_1 + 2P_2$ is at most $s - 1$.

Suppose now that $u_1, \ldots, u_s$ are any set of linearly independent columns of $I - P_1$ where one of these vectors was used as the vector u in forming $P_1 + 2P_2$. Without loss of generality, suppose that $u = u_1$. Then, for any set of scalars $\beta_2, \ldots, \beta_s$, the vectors

$$u_i + \beta_i u_1, \qquad i = 2, \ldots, s,$$

are linearly independent, and, since $vu = vu_1 \neq 0$, taking

$$\beta_i = -(vu_1)^{-1} vu_i, \qquad i = 2, \ldots, s,$$

gives

$$(P_1 + 2P_2)(u_i + \beta_i u_1) = -u_i - \beta_i u_1,$$

so that the signature of $P_1 + 2P_2$ is at least $s - 1$.

A proof of the dual relationship follows in much the same manner. For if $P_1 - 2P_2$ is involutory and $P_2^2 = P_2$, then

$$P_1P_2 = P_2P_1 = P_2 \tag{4.2}$$

by Theorem 5(ii), so that rows and columns of P_2 must be left and right eigenvectors of P_1, respectively, for $\lambda = 1$. Then forming an idempotent matrix $P_2 = (vu)^{-1}uv$ of rank one with u a column and v a row of $I + P_1$ chosen as before, P_2 satisfies (4.2) and $P_2u = u$. Also, for any eigenvector x of P_1 for $\lambda = -1$, we have $P_2x = 0$ from (4.2), so that $(P_1 - 2P_2)x = -x$, and in addition $(P_1 - 2P_2)u = -u$. Hence the signature of $P_1 - 2P_2$ is $s + 1$, since a similar argument shows the signature of $P_1 - 2P_2$ is at most $s + 1$. ■

Although decreasing the signature of an involution P_1 with maximum signature or increasing the signature of an involution P_1 with minimum

signature is not included in the statement of Theorem 9, this can be accomplished in a similar manner by using the Levine-Nahikian theorem. For if P_1 has signature $s = n$, then $P_1 = -I_n$. Choose u to be any nonzero column vector and v to be any nonzero row vector such that $vu = 1$. Then $-I_n + 2uv$ is an involution of signature $n - 1$, as $v(2u) = 2$. Moreover uv is idempotent of rank one. Similarly, if P_1 has signature 0, then $P_1 = I$, and for such a u and v as before, $I - 2uv$ is an involution of signature one.

For involutions P_1 over fields of characteristic $p = 2$, we have $I - P_1 = I + P_1$, so that the procedure employed in Theorem 9 cannot be used directly to change the signature. The analogs of Theorem 9 to change the signature are given in Theorem 10 and Theorem 11, but the proofs are somewhat more complicated.

THEOREM 10. *Let P_1 be an arbitrary n by n involution with signature s, $0 < s \leqslant [n/2]$, over any field of characteristic $p = 2$. Then there exists at least one matrix P_2 with rank one and $P_2^2 = 0$ such that $P_1 + P_2$ is involutory and the signature of $P_1 + P_2$ is $s - 1$. Such a P_2 may be obtained by setting $P_2 = (v_k)^{-1}uv$, where v is any nonzero row of $I + P_1$, say the ith, and u is any column of $I + P_1$, say the kth, for which the ith component of u, that is, the kth component v_k of v, is nonzero.*

Proof. Since P_1 is an n by n involution with signature s, the canonical form J for P_1 given in Section 2 implies that P_1 has $n - s$ simple eigenvectors x_i satisfying

$$P_1 x_i = x_i \tag{4.3}$$

and s generalized eigenvectors y_j satisfying

$$P_1 y_j = y_j + x_j, \tag{4.4}$$

where x_j is the simple eigenvector associated with y_j for $j = 1, \ldots, s$ and $\{x_i : 1 \leqslant i \leqslant n - s\} \cup \{y_j : 1 \leqslant j \leqslant s\}$ is a linearly independent set of n vectors. Since $P_1(I + P_1) = I + P_1$, it follows that any nonzero column of $I + P_1$ can be used as an eigenvector x_i in (4.3) and $I + P_1 \neq 0$ as $s > 0$.

Designate the columns of P_1 as z_k, $k = 1, \ldots, n$, and let e_k, $k = 1, \ldots, n$, denote the columns of I, so that any column u of $I + P_1$ can be written as

$$u = e_k + z_k \tag{4.5}$$

for some $k = 1, \ldots, n$. Notice that $z_k \neq 0$, since P_1 is invertible, and hence $u \neq e_k$. In addition, let v be any nonzero row of $I + P_1$ with components $v_1, \ldots, v_n$. Then with u any nonzero vector in (4.5) and α any nonzero scalar, $P_2 = \alpha uv$ has rank one and $P_2^2 = 0$, since $(I + P_1)^2 = 0$, and thus $vu = 0$. Moreover, $P_1 P_2 = P_2 P_1 = P_2$ for any such choice of u, v, and α, so that $P_1 + P_2$ is involutory by Theorem 6(ii).

Also, observe that $P_1 e_k = z_k$ and therefore $P_1 z_k = e_k$. In addition, e_k and z_k are generalized eigenvectors of P_1 associated with simple eigenvector u of P_1, since

$$\begin{aligned} P_1 e_k &= z_k = e_k + e_k + z_k = e_k + u, \\ P_1 z_k &= e_k = e_k + z_k + z_k = u + z_k. \end{aligned} \tag{4.6}$$

Now for any component $v_k \neq 0$ of v, $ve_k = v_k \neq 0$. As in Theorem 9, choose u to be a column of $I + P_1$ containing a $v_k \neq 0$ and set $P_2 = (ve_k)^{-1} uv$. Thus for an eigenvector x_i of P_1 in (4.3), $(I + P_1)x_i = 0$, so that $vx_i = 0$, which yields

$$\left(P_1 + (ve_k)^{-1} uv\right) x_i = x_i.$$

Hence every eigenvector in (4.3) is also an eigenvector of $P_1 + P_2$, and in particular, u is such an eigenvector. Using (4.5), however,

$$\begin{aligned} \left\{P_1 + (ve_k)^{-1} uv\right\} e_k &= \left\{P_1 + (ve_k)^{-1} (e_k + z_k) v\right\} e_k \\ &= z_k + e_k + z_k = e_k, \end{aligned}$$

and thus e_k is a simple eigenvector of $P_1 + P_2$. Consequently, the generalized eigenvector e_k of P_1 is a simple eigenvector of $P_1 + P_2$. Since we may assume that $x_1 = u$ and $y_1 = e_k$, the set $\{x_i : 1 \leqslant i \leqslant n - s\} \cup \{y_1\}$ is linearly independent and contains $n - s + 1$ simple eigenvectors of $P_1 + P_2$. Therefore, the signature of $P_1 + P_2$ is at most $s - 1$. Moreover, for any $j = 2, \ldots, s$,

$$(P_1 + P_2)\left\{x_j + (ve_k)^{-1} (vy_j) u\right\} = x_j + (ve_k)^{-1} (vy_j) u$$

and

$$\begin{aligned} (P_1 + P_2)\left\{y_j + (vy_j) e_k\right\} &= \left\{P_1 + (ve_k)^{-1} uv\right\}\left\{y_j + (vy_j) e_k\right\} \\ &= x_j + y_j + (ve_k)^{-1} uvy_j + (vy_j) e_k \\ &= \left\{y_j + (vy_j) e_k\right\} + \left\{x_j + (ve_k)^{-1} (vy_j) u\right\}. \end{aligned}$$

Since $\{x_j+(ve_k)^{-1}(vy_j)u: j=2,\ldots,s\}\cup\{y_j+(vy_j)e_k: j=2,\ldots,s\}$ is linearly independent, the signature of P_1+P_2 is at most $s-1$. Hence the signature of P_1+P_2 is $s-1$. ■

We now show how to increase the signature of an involution when the characteristic of the field is 2. As shown in Theorem 11, the difficulty in this case is that the vectors u and v used to form P_2 in Theorem 10 cannot be obtained from rows and columns of $I+P_1$, but must be determined in a different manner.

THEOREM 11. *Let P_1 be an arbitrary matrix over any field of characteristic $p=2$ with $P_1^2=I$ and signature s, $0\leqslant s<[n/2]$. Then there exists at least one matrix P_2 of rank one with $P_2^2=0$ such that P_1+P_2 is involutory and the signature of P_1+P_2 is $s+1$. Such a $P_2=uv$ may be formed by setting u equal to the sum of two properly chosen simple eigenvectors of P_1 and choosing v in the solution set of a linear system of equations whose coefficient matrix is constructed from P_1 and certain simple eigenvectors of P_1.*

Proof. If $s=0$, then $P_1=I$, and for any nonzero column vector u and nonzero row vector v with $vu=0$, $P_2=uv$ has rank one, $P_2^2=0$, and $I+P_2$ is an involution with signature 1 by the second Levine-Nahikian theorem.

Now assume that $1\leqslant s<[n/2]$. Then $n\geqslant 4$ and $r=n-2s\geqslant 2$. From (4.6) each nonzero column of $I+P_1$ is a simple eigenvector of P_1 associated with a generalized eigenvector of P_1 and is an element of the null space of $I+P_1$. Moreover, as P_1 is similar to the canonical form J in Section 2, $I+P_1$ is similar to $I+J$, and hence $I+P_1$ has rank s. Thus any simple eigenvector of P_1 associated with a generalized eigenvector of P_1 must be a linear combination of the columns of $I+P_1$. As $r\geqslant 2$, P_1 has at least two linearly independent simple eigenvectors x_1 and x_2 which are not associated with any generalized eigenvector of P_1. Moreover, x_1+x_2 is also such a simple eigenvector of P_1. In particular, as the dimension of the null space of $I+P_1$ is $n-s\geqslant s+2$, x_1 and x_2 may be chosen to be linearly independent vectors in the null space of $I+P_1$ which are not in the column space of $I+P_1$. Now let x_i, $i=1,\ldots,n-s$, be simple eigenvectors of P_1, and y_j, $j=1,\ldots,s$, be generalized eigenvectors of P_1, where

$$P_1y_j=y_j+x_{n-2s+j}$$

for $j=1,\ldots,s$ and $\{x_1,\ldots,x_{n-s},y_1,\ldots,y_s\}$ is linearly independent. Let $X=[x_3,\ldots,x_{n-2s}]$, i.e., the matrix whose columns are the linearly independent simple eigenvectors $x_3,\ldots,x_{n-2s}$ of P_1 which are not associated with any

generalized eigenvector of P_1. Thus the partitioned matrix $[I + P_1, X, x_1, x_2]$ has rank $n - s < n$, and the system of equations

$$v[I + P_1, X, x_1, x_2] = [0, 1, 1],$$

where 0 denotes the null row vector with $2n - 2s - 2$ components, has a nontrivial solution v. But for any such $v \neq 0$, $v(x_1 + x_2) = 0$, so that if $u = x_1 + x_2$, then $P_2 = uv$ has rank one and $P_2^2 = 0$. Moreover, as $vP_1 = v$, $P_1 + P_2$ is an involution by Theorem 6(ii). Finally, since

$$\{P_1 + (x_1 + x_2)v\}(x_1 + x_2) = x_1 + x_2$$

and

$$\{P_1 + (x_1 + x_2)v\}x_1 = x_1 + (x_1 + x_2),$$

x_1 is a generalized eigenvector of $P_1 + P_2$ associated with the simple eigenvector $x_1 + x_2$ of $P_1 + P_2$. Also, for any generalized eigenvector y_j of P_1 with $P_1 y_j = y_j + x_{n-2s+j}$,

$$\{P_1 + (x_1 + x_2)v\}y_j = y_j + \{x_{n-2s-j} + (vy_j)(x_1 + x_2)\}$$

and

$$\{P_1 + (x_1 + x_2)v\}\{x_{n-2s+j} + (vy_j)(x_1 + x_2)\} = x_{n-2s+j} + (vy_j)(x_1 + x_2).$$

The second equation follows because $(I + P_1)y_j = x_{n-2s+j}$ and $v(I + P_1) = 0$ implies $vx_{n-2s-j} = 0$. Thus for this choice of P_2, since $\{x_1\} \cup \{y_j: j = 1, \ldots, s\}$ is linearly independent, $P_1 + P_2$ has signature $\geq s + 1$. Moreover, for any x_i, $i = 3, \ldots, n - 2s$, $vx_i = 0$ and hence x_i is a simple eigenvector of $P_1 + P_2$. As $\{x_1 + x_2\} \cup \{x_{n-2s-j} + (vy_j)(x_1 + x_2): j = 1, \ldots, s\} \cup \{x_i: i = 3, \ldots, n - 2s\}$ is linearly independent, $P_1 + P_2$ has signature $s + 1$. ■

Theorem 9 can be used to construct a complete set of $n + 1$ dissimilar involutions when the characteristic $p \neq 2$, and the choice of a first involution P_1 is arbitrary. In the case of a field of characteristic $p = 2$, Theorems 10 and 11 can be used to construct a complete set of $1 + [n/2]$ dissimilar involutions with the first involution P_1 again arbitrary, but if it is necessary to both increase and decrease the signature of P_1, the construction methods are quite different. In either case, however, the process provides a simple computational

procedure for constructing dissimilar involutions which does not require starting with I or solving $P_2Q_2 = 2I_s$ or $P_2Q_2 = 0$ in order to construct H in (2.1) or (2.3), both of which are required in the Levine-Nakihian construction. Such procedures are illustrated by numerical examples in Section 5.

To conclude this section we observe that given any n by n involution $P_1 \neq \pm I_n$ with signature s, a new involution with signature s can be constructed from P_1. If P_1 is an involution of signature s, $0 < s < n$, over a field of characteristic $p \neq 2$, v is any nonzero row of $I - P_1$, u is any nonzero column of $I + P_1$, and α is any nonzero scalar, then the matrix $P_2 = \alpha uv$ has rank one and satisfies $P_2^2 = 0$ and $P_1P_2 + P_2P_1 = 0$. Thus $P_1 + P_2$ is an involution by Theorem 6(ii). In this case, however, it is seen at once that for any vector x with $P_1x = x$, $(P_1 + P_2)x = x$, and for any vector y with $yP_1 = -y$, $y(P_1 + P_2) = -y$. Consequently, P_1 and $P_1 + P_2$ have the same signature, and it follows that this variation on the method of choosing vectors u and v in Theorem 9 can be used to construct pairs of involutions for which the signature does not change. Clearly, the same conclusion holds when v is any nonzero row of $I + P_1$ and u is any nonzero column of $I - P_1$. One should also observe, however, that if u and v are chosen as in the proof of Theorem 9, but $vu = 0$, then for $P_2 = \pm 2\alpha uv$, P_1 and P_2 do not satisfy condition (ii) of Theorem 6 and hence $P_1 + P_2$ is not an involution. The analog of these observations in a field of characteristic $p = 2$ is seen by noting that if P_1 is any n by n involution with signature s, $0 < s \leqslant [n/2]$, then the results and notation in the first and second paragraphs of the proof of Theorem 10 are applicable, and with v any nonzero row of $I + P_1$, $u = e_k + z_k$ any nonzero column of $I + P_1$ such that $ve_k = 0$, α any nonzero scalar, and $P_2 = \alpha uv$, we have that $P_1 + P_2$ is an involution. Moreover, e_k is a generalized eigenvector of P_1 with associated simple eigenvector u. Again the simple eigenvectors x_i in (4.3) are simple eigenvectors of $P_1 + P_2$. As before, we may assume $x_1 = u$ and $y_1 = e_k$. Then for any $j = 1, \ldots, s$,

$$(P_1 + P_2)\{x_j + \alpha(vy_j)u\} = x_j + \alpha(vy_j)u$$

and

$$(P_1 + P_2)y_j = y_j + x_j + \alpha(vy_j)u.$$

As $ve_k = 0$ and $y_1 = e_k$, the set of vectors

$$\{x_j + \alpha(vy_j)u : j = 1, \ldots, s\} \cup \{x_i : i = s + 1, \ldots, n - s\} \cup \{y_j : j = 1, \ldots, s\}$$

is linearly independent, and hence $P_1 + P_2$ has signature s.

5. NUMERICAL EXAMPLES

To illustrate the computational procedures provided by Theorems 9, 10, and 11, we begin with the involutions constructed by Levine and Nahikian [1].

Using our notation, let P_1 be the involution

$$P_1 = \begin{bmatrix} 3 & 6 & -11 & 14 & -4 \\ -4 & -7 & 13 & -8 & 0 \\ 2 & 3 & 4 & -1 & 2 \\ -2 & -3 & -3 & 2 & -2 \\ -2 & -3 & -3 & 1 & -1 \end{bmatrix}$$

over the field of integers mod 29, where signature$(P_1) = 2$. Then the matrices

$$I - P_1 = \begin{bmatrix} -2 & -6 & 11 & -14 & 4 \\ 4 & 8 & -13 & 8 & 0 \\ -2 & -3 & -3 & 1 & -2 \\ 2 & 3 & 3 & -1 & 2 \\ 2 & 3 & 3 & -1 & 2 \end{bmatrix}$$

and

$$I + P_1 = \begin{bmatrix} 4 & 6 & -11 & 14 & -4 \\ -4 & -6 & 13 & -8 & 0 \\ 2 & 3 & 5 & -1 & 2 \\ -2 & -3 & -3 & 3 & -2 \\ 2 & -3 & -3 & 1 & 0 \end{bmatrix}$$

can be used to construct idempotent matrices P_2 in Theorem 9. For example, taking v as the first row of $I - P_1$ and u as the first column, then computing mod 29 gives $vu = -4$, so

$$2P_2 = 2(-22)uv = \begin{bmatrix} -2 & -6 & 11 & -14 & 4 \\ 4 & 12 & -22 & 28 & -8 \\ -2 & -16 & 11 & -14 & 4 \\ 2 & 6 & -11 & 14 & -4 \\ 2 & 6 & -11 & 14 & -4 \end{bmatrix},$$

and it follows from Theorem 5 that

$$P_1+2P_2=\begin{bmatrix}1&0&0&0&0\\0&5&-9&20&-8\\0&-3&15&-15&6\\0&3&-14&16&-6\\0&3&-14&15&-5\end{bmatrix} \tag{5.1}$$

is an involution, and the signature of P_1+2P_2 is 1 by Theorem 9. In a similar manner, use the first row and last column of $I+P_1$ to form vectors v and u. Then $vu=-8$ and

$$2P_2=2(18)uv=\begin{bmatrix}-25&-23&18&-15&25\\0&0&0&0&0\\27&26&-9&22&-27\\-27&-26&9&-22&27\\0&0&0&0&0\end{bmatrix}$$

to give the involution

$$P_1-2P_2=\begin{bmatrix}28&0&0&0&0\\-4&-7&13&-8&0\\-25&-23&13&-23&0\\25&23&-12&24&0\\-2&-3&-3&1&-1\end{bmatrix}, \tag{5.2}$$

where the signature of P_1-2P_2 is 3. It should be noted that applying the method for decreasing the signature to P_1+2P_2 in (5.1) then gives I, whereas two applications of the method for increasing the signature, starting with P_1-2P_2 in (5.2), give $-I$.

To illustrate the method for constructing involutions for matrices in a field of characteristic $p=2$, let P_1 be the involution

$$P_1=\begin{bmatrix}0&0&1&1&0\\1&0&0&1&1\\1&1&1&1&1\\0&1&1&1&1\\0&0&0&0&1\end{bmatrix},$$

where the signature of P_1 is 2. Then

$$I + P_1 = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

and using the first row and first column of $I + P_1$ to form

$$P_2 = uv = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

gives the involution

$$P_1 + P_2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \tag{5.3}$$

from Theorem 6, where the signature of $P_1 + P_2$ is 1, by Theorem 10. As in the case of $P_1 + 2P_2$ in (5.1), now reducing the signature of $P_1 + P_2$ in (5.3) again gives I.

To show the method of increasing the signature for the case $p = 2$, let P_1 be the involution

$$P_1 = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}$$

with signature 1. Then $x_1 = [1\ 1\ 0\ 0\ 0\ 0]^T$, $x_2 = [1\ 0\ 1\ 0\ 0\ 0]^T$, $x_3 = [1\ 0\ 0\ 1\ 0\ 0]^T$, $x_4 = [1\ 0\ 0\ 0\ 1\ 0]^T$, and $x_5 = [1\ 1\ 1\ 1\ 1\ 1]^T$ are linearly independent simple eigenvectors of P_1, and $y_1 = [1\ 0\ 0\ 0\ 0\ 0]^T$ is a generalized eigenvector of P_1 with associated simple eigenvector x_5. Then

$v = [0\ 1\ 1\ 0\ 0\ 0]^T$ is a solution of $v[I + P_1, x_3, x_4, x_1, x_2] = [0, 1, 1]$, where 0 is the null row vector with 8 components. Thus

$$P_2 = (x_1 + x_2)v = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

and hence

$$P_1 + P_2 = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 \end{bmatrix} \tag{5.4}$$

is an involution from Theorem 6, where signature of $P_1 + P_2$ is 2, by Theorem 11. If this method is now applied to the involution in (5.4), an involution

$$\begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}$$

of signature 3 is obtained when the basis specified in the proof of Theorem 11 is used.

The authors wish to thank the referee for the helpful suggestions and a detailed list of references.

REFERENCES

1 J. V. Brawley, Similar involutory matrices (mod p^m), *Amer. Math. Monthly* 73:499–501 (1966).

2 J. V. Brawley, Similar involutory matrices modulo R, *Duke Math. J.* 34:649–666 (1967).

3 J. V. Brawley, Certain sets of involutory matrices and their groups, *Duke Math. J.* 36:473–478 (1969).
4 J. V. Brawley and R. O. Gamble, Involutory matrices over finite commutative rings, *Linear Algebra Appl.* 21:175–188 (1978).
5 J. V. Brawley and Jack Levine, Equivalence classes of involutory mappings, *Duke Math. J.* 39:211–217 (1972).
6 J. D. Fulton, Symmetric involutory matrices over finite fields and modular rings of integers, *Duke Math. J.* 36:401–408 (1979).
7 L. S. Hill, Concerning certain linear transformation apparatus in cryptography, *Amer. Math. Monthly* 38:135–154 (1931).
8 J. H. Hodges, The matrix equation $X^2 - I = 0$ over a finite field, *Amer. Math. Monthly* 65:518–520 (1958).
9 N. A. Khan, On involutory matrices, *Amer. Math. Monthly* 63:704–709 (1956).
10 Jack Levine, Variable matrix substitution in algebraic cryptography, *Amer. Math. Monthly* 65:170–179 (1958).
11 Jack Levine, Some elementary cryptoanalysis of algebraic cryptography, *Amer. Math. Monthly* 68:411–418 (1961).
12 Jack Levine, Analysis of the case $n = 3$ in algebraic cryptography with involutory key-matrix and known alphabet, *J. Reine Angew. Math.* 213:1–30 (1963).
13 Jack Levine and J. V. Brawley, Involutory commutants with some applications to algebraic cryptography I, *J. Reine Angew. Math.* 224:20–43 (1966); II, *J. Reine Angew. Math.* 227:1–24 (1967).
14 Jack Levine and R. R. Korfhage, Automorphisms of Abelian groups induced by involutory matrices, *Duke Math. J.* 29:631–646 (1962).
15 Jack Levine and R. R. Korfhage, Automorphisms of Abelian groups induced by involutory matrices, modulo $p > 2$, *Duke Math. J.* 30:161–170 (1963).
16 Jack Levine and R. R. Korfhage, Automorphisms of Abelian groups induced by involutory matrices, general modulus, *Duke Math. J.* 31:631–654 (1964).
17 Jack Levine and H. M. Nahikian, On the construction of involutory matrices, *Amer. Math. Monthly* 65:267–272 (1962).
18 J. C. Perkins and J. D. Fulton, Symmetric involutions over fields of characteristic 2, *Duke Math. J.* 38:697–702 (1971).
19 Irma Reiner, The matrix congruence $X^2 \equiv I \pmod{p^n}$, *Amer. Math. Monthly* 67:773–775 (1960).

Received 13 September 1982; revised 25 March 1983